

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

1640 North Taylor Drive, Unit B, Sheboygan, WI, including any storage or outbuildings and garages and a black 2019 Ford Escape, with WI registration plate 656UGZ, Vin # 1FMCU9HD9KUA00017, as further described on Attachment A

Case No. 24-M-491 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

10-8-24

YOU ARE COMMANDED to execute this warrant on or before _____ (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 9-24-24. 4:30 pm

Judge's signature

City and state: Milwaukee, WI

Honorable **Stephen C Dries** Magistrate Judge
Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED:

The entire premises located at 1640 N. Taylor Drive, Unit B, Sheboygan, Wisconsin ("SUBJECT PREMISES"), including any storage or outbuildings and garages, more particularly described as a two-story apartment building, located in the City of Sheboygan, Wisconsin, Sheboygan County, with various shades of brown bricks and white siding, white trim surrounding the exterior windows, white gutters, and dark gray shingles. The front of the apartment faces north east, and the apartment's address "1640" is affixed on four white tiles with units "1640A", "1640B", "1640C", and "1640D" on the east corner of the building and faces to the southeast towards N. Taylor Drive. The front entrance of the SUBJECT PREMISES has a white exterior door with a window. Once inside the front white door, the common area opens up to other units, and immediate to the left is a brown painted door at the bottom of the stairs with brown wood trim, with the letter "B" attached to the upper center of the door. There is an exterior parking lot on the east side of the building. The SUBJECT PREMISES is approximately one tenth of one mile to the north of West Meadows Court and is located on the west side of N. Taylor Drive in the City of Sheboygan.

A black 2019 Ford Escape, with Wisconsin registration plates 656UGZ, which is registered to NOLAN PITTSCH. The Ford Escape has a VIN # of 1FMCU9HD9KUA00017 and has been observed in the parking lot of 1640 N. Taylor Drive, Sheboygan, Wisconsin. Pictures of the residence and vehicle are provided below.







ATTACHMENT B

ITEMS TO BE SEIZED:

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, 18 U.S.C. §§ 2251(a) Sexual Exploitation of a minor/"production" of CSAM and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography):

1. Computers or storage media used to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- A. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- B. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

C. Evidence of the lack of such malicious software;

D. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

E. Evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

F. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

G. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

H. Evidence of the times the COMPUTER was used;

I. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

J. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

K. Records of or information about Internet Protocol addresses used by the COMPUTER;

L. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or

“favorite” web pages, search terms that the user entered in any Internet search engine, and records of user-typed web addresses; and

M. Contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

A. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

B. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

C. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as

microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) and hold up the device(s) to the face of individuals found at the premises to the Touch ID sensor of Android or Apple brand device(s) and the camera of the Apple brand devices, smartphones, or tablets, such as an iPhone or iPad, found at the premises for the purposes of attempting to unlock the device(s) via Touch ID and Face ID in order to search the contents as authorized by this warrant.

Sep 24, 2024

s/ Mariah Kauder

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*1640 North Taylor Drive, Unit B, Sheboygan, WI, including any storage or
outbuildings and garages and a black 2019 Ford Escape, with WI
registration plate 656UGZ, Vin # 1FMCU9HD9KUA00017,
as further described on Attachment A

Case No. 24-M-491 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the
property to be searched and give its location)*:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the
person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

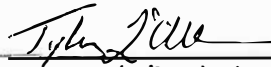
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2251(a);	Sexual Exploitation of a minor - production
18 U.S.C. § 2252(A)(5)(B)	Possession of and access with intent to view child pornography

The application is based on these facts:
See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Tyler L'Allier, TFO - HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ *(specify reliable electronic means)*.

Date: 9-24-24



Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Tyler L'Allier, being duly sworn, hereby state as follows:

INTRODUCTION

1. I am a Task Force Officer (TFO) with the Department of Homeland Security, Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a Special Agent with HSI since August 2024. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin.

2. My experience as an HSI TFO and Washington County Detective have included the investigation of cases involving the use of computers and the Internet to commit violations of federal law involving child exploitation, including the production, transportation, receipt, distribution and possession of child pornography. I have received training and have gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications and the execution of searches and seizures involving computer crimes. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2251, 2252 and 2252A.

3. I am responsible for investigating violations of federal laws, including the offenses of advertisement, production, transportation, receipt, distribution, and possession of child pornography, (as defined in Title 18, United States Code Section 2256), in interstate or foreign commerce by any means, including by computer.

4. The statements contained within this affidavit are based on my training and experience as well as the training and experience of and information communicated to me by other law enforcement personnel with whom I have personally spoken or communicated via email.

5. This affidavit is made in support of an application for a warrant to search: The entire premises located at 1640 N. Taylor Drive (Unit B), Sheboygan, Wisconsin ("SUBJECT PREMISES"), including any storage or outbuildings and garages, more particularly described as a two-story apartment building, located in the City of Sheboygan, Wisconsin, Sheboygan County, with various shades of brown bricks and white siding, white trim surrounding the exterior windows, white gutters, and dark gray shingles. The front of the apartment faces northeast, and the apartment's address "1640" is affixed on four white tiles with units "1640A", "1640B", "1640C", and "1640D" on the east corner of the building and faces to the southeast towards N. Taylor Drive. The front entrance of the SUBJECT PREMISES has a white exterior door with a window. Once inside the front white door, the common area opens up to other units, and immediate to the left is a brown painted door at the bottom of the stairs with brown wood trim, with the letter "B" attached to the upper center of the door. There is an

exterior parking lot on the east side of the building. The SUBJECT PREMISES is approximately one tenth of one mile to the north of West Meadows Court and is located on the west side of N. Taylor Drive in the City of Sheboygan. A black in color 2019 Ford Escape (VIN: 1FMCU9HD9KUA00017) with Wisconsin registration plate 656UGZ that is registered to Nolan Marshall Pitsch (white male, date of birth 1/5/1994) that has been observed on numerous occasions parked in the parking lot at 1640 N. Taylor Drive.

6. The statements in this affidavit are based in part on information provided by a TFO for HSI, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (sexual exploitation of a minor/"production" of CSAM); and 18 U.S.C. § 2252A(a)(5)(B) (possession of and access with intent to view child pornography), are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

7. In my capacity as an investigator of criminal violations relating to child exploitation and child pornography, I have become familiar with the following federal statutes:

a. Production of Child Pornography, 18 U.S.C. §§ 2251(a), which prohibits any person from employing, using, persuading, inducing, enticing, or

coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct.

b. Receipt and Distribution of Child Pornography, 18 U.S.C. § 2252A(a)(2)(A), which makes it unlawful for someone to knowingly receive or distribute any child pornography that has been mailed or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. Possession of Child Pornography, 18 U.S.C. § 2252A(a)(5)(B), which makes it unlawful for someone to knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. Pursuant to 18 U.S.C. § 2256(8), Child Pornography is defined as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where -

(A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (B) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.”

e. Pursuant to 18 U.S.C. § 2256(1), the term “minor,” is defined as “any person under the age of eighteen years.”

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Chat room,” as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image of picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

f. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. “Hash Value” refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a “digital fingerprint” for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes.

i. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their

customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

m. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

n. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

o. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or

opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

p. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

q. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**BACKGROUND ON NATIONAL CENTER FOR
MISSING AND EXPLOITED CHILDREN**

9. Based on my training and experience, and publicly available information, I know that the National Center for Missing and Exploited Children (NCMEC) is a nonprofit organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

10. In addition to reports from the general public, reports are made by U.S. electronic communication service (ECS) providers and remote computing services (RCS), which are required by 18 U.S.C. § 2258A to report “apparent child pornography”

to NCMEC via the CyberTipline if they become aware of the content on their servers. Specially trained analysts, who examine and evaluate the reported content, review leads, add related information that may be useful to law enforcement, use publicly available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

11. The CyberTipline receives reports, known as CyberTips, about the possession, production and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

12. The CyberTip reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an ECS or RCS uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography.

SUMMARY OF INVESTIGATION

13. On August 26, 2024, the HSI - Albany, New York field office was contacted by the mother of a 13-year-old minor victim (MV1), regarding sexual exploitation via interstate communications that included the direction and production of child sex abuse material (CSAM) with her daughter by an individual believed to be in Wisconsin. HSI - Albany researched phone numbers that the minor victim communicated with, and identified a potential suspect as Nolan Marshall Pitsch (white male, date of birth 1/5/1994). MV1's mother spot checked her child's phone, and located disturbing messages of a sexual nature, and text messages including CSAM between the victim and a subject identified as "Nate." MV1 identified the suspect as, "Nate," and stated they met him on TikTok. A photograph in the messages was located, and MV1's sister did research to find out that the individual that was in a photo that traced back to a Facebook account belonging to Steve Pitsch. HSI Special Agent (SA) Cecilione viewed the photograph and recognized it to display the case target, Nolan Pitsch. HSI Albany conducted a Cellebrite extraction of MV1's devices, and observed CSAM material on the device used to communicate with Pitsch, corroborating the allegation.

14. On August 30, 2024, I was assigned this case, and reviewed all available documentation in the coming days, including that from HSI - Albany field office, and a CyberTip that was generated, #196968626. The CyberTip listed Nolan Pitsch as the

suspect, with phone number (920) 627-1085, email npitsch085@gmail.com, and snapchat username: "papers34678."

15. Several administrative subpoenas were submitted for snapchat username "papers34678," gmail account: npitsch085@gmail.com, IP addresses 71.86.236.218 (Charter) and 166.181.84.215 (Wireless Data Service Provider Corporation), phone numbers (920) 627-1085 (US Cellular) and (608) 424-5302 (Textnow), and TikTok for username "@np851234."

16. I conducted further background into the suspect, Nolan Pitsch. He has a Facebook account located at <https://www.facebook.com/nmpitsch>, and an X (formally known as Twitter) account: "@NolanMP94." Nolan is employed by Marcus Theatres in Sheboygan as a box office cashier.

17. I reviewed text messages sent between MV1's cellular device and the suspect. These messages spanned from August 16, 2024, through August 24, 2024, and were extremely sexually graphic in nature, as the suspect specified sex acts, he wanted to perform on MV1. The messages started between MV1 and the suspect's number of (608) 424-5302, that was verified to be a Textnow number. On August 16, 2024, he sent a message to MV1: "Then you get on your knees & suck on cock & taste all the pussy juices. I rub your clit while you're sucking on my cock. I have you massage your tits, while you suck on my dick hands free." This was followed up with a .jpg image (: files\Image\PART_1723843976040_dd4e5b05-7d30-42d2-8189-65594b48de68.jpg) being sent to the suspect. Several minutes later, the suspect continues to state: "Then I grab

you & flip you over & shove you on the bed. I grab your hips & start to finger both your pussy & asshole at the same time. As I'm doing that, I use the pussy juices to lube up your asshole. Then as I'm fingering your asshole, I slip in 2 fingers & keep stretching it. Then you beg daddy for the real thing in your asshole. You grab both ass cheeks & I press the tip against your asshole. I tell you to take a deep breath. You breathe in & my cock slowly enters the inside of your tightly fresh asshole. You tell daddy to speed up but I tell you take your time & let it get harder inside of you. So i start to speed up. I start thrusting & grab your hips & spank your ass." MV1 refers to the suspect as, "daddy," and said that he earned three pics of "Tit's and ass." MV1 then sends the suspect two more images (files\Image\PART_1723846131246_60ea3fd4-cbc4-4559-9912-11209763ed56.jpg and files\Image\PART_1723846187636_8fbc6e4e-df3d-493b-ab89-1eaa98dca33c.jpg). Several hours later, the suspect requests that she sends him a full naked, "speak pose", with, "... feet with legs spread to see pussy & tits with face showing." MV1 asks the suspect to find an example online and send it to her. The suspect continues to request photos of specific angles, poses, and genitalia being shown. He tells her, "I'll shove you on the bed & make sure you stay naked & I'll shove my cock down down your throat to hold you down."

18. On August 17, 2024, the suspect later requested that MV1 send images and videos to his other number, (920) 627-1085, that was confirmed to be US Cellular, and listed to his father. His reasoning was that image and video quality were higher.

The 1085 number was confirmed to be a current US Cellular number, and lists back to the suspect, Nolan Pitsch, when checking Accurint.

19. The suspect tells MV1, "I love you," and continued to request specific images and videos of her in sexual poses. It also appeared that the suspect provided several .jpg images to MV1 of what the conversation leads me to believe is a penis. MV1 raises concerns that she is getting attached to the suspect, and references that he doesn't even go to their school, confirming the fact that the suspect is feigning as a juvenile. Conversation continues and the suspect asks her other sexually descriptive questions, such as how many guys she could take "fucking her at once," "What's your dating age range?", "Would you fuck over 18?" "20 & older?", and asks her if her dogs, "Would they lick your pussy? If it was out." The suspect would highlight requests of certain body parts in different messages, requesting the bottom of her feet, focusing on the "asshole". He also requested a video of MV1 urinating, with her exposed genitals. MV1 was confirmed to be a 13-year-old child victim. In the text exchanges MV1 stated she was 13 and this was confirmed during the initial investigation conducted by HSI - Albany.

20. On 08/21/2024 at 9:14:57 PM (UTC-4), the suspect directs MV1 to "Flash Daddy." At 9:16:25 PM (UTC-4), MV1 sends the suspect a photo, image filename: f7a7844d-3d31-4ac8-b147-aa175097bc44.jpg. The image was taken in the bathroom by MV1. MV1 is standing next to a toilet and a bathtub, standing on what appears to be a towel on the floor. MV1 arms are out in front of her, and she appears to be taking the

photograph. MV1 is completely naked from the neck down exposing her underdeveloped breasts. The hair on the top of her pubic area can be seen, but not her vaginal area. The image as described above are CSAM. After sending the image MV1 states she is going to take a shower. The suspect texts, "Show another angle 😊" and MV1 sends another photograph. The suspect directs MV1 to sit on the edge of the toilet and show the pussy with tits and to sneak in the face but MV1 says, "No I'm taking my shower."

21. The above described messages are in direct violation of Sexual exploitation of a minor/"production" of CSAM (18 U.S.C. § 2251 (a)). The suspect, used, persuaded, induced, or enticed a minor to engage in sexually explicit conduct for the purpose of producing visual depictions of such conduct, and the depictions produced were transmitted interstate.

22. The above-described messages are in direct violation of Possession of and access with intent to view child pornography (18 U.S.C. § 2252A(a)(5)(B)). The suspect knowingly possesses or accessed with intent to view child pornography, depicts actual minors engaged in sexually explicit conduct, and is aware of the sexually explicit nature and character of the materials and that visual depictions are of minors engaged in sexually explicit conduct. Nolan Pitsch asked MV1 her age, and MV1 confirmed that it was 13 years old, prior to requesting and receiving the images from MV1.

23. On September 4, 2024, I contacted the Wisconsin Department of Justice ICAC Task Force and requested that CyberTip #196968626 be assigned to me as it is

associated with HSI – Albany, New York field office initial investigation. The CyberTip listed the Primary Incident Type as Online Enticement of Child for Sexual Acts and has an incident date of 06-06-2024 at 21:05:14 UTC. The CyberTip was received by NCMEC on 07-27-2024 at 12:43:09 UTC. The reporting Electronic Service Provider (ESP) is Snapchat.

24. The listed child victim has a listed Date of Birth of 05-05-2009, which would make the child victim 15 years old. The associated email address for the child victim is just4lieke@att.net and the Screen/Username is liekelewis.

25. The additional information reported by Snapchat states the account name in the CyberTip submission was engaged in the sextortion of a minor.

26. The following snap messages were exchanged between liekelewis and papers34678 and are listed in the CyberTip:

- a. liekelewis 2024-06- 05T01:54:34.513Z: nothin
- b. liekelewis 2024-06-05T01:54:37.072Z: wbu
- c. papers34678 (Reported) 2024-06-05T02:32:30.963Z: I have a question
- d. liekelewis 2024-06-05T14:43:22.519Z: alr go ahead
- e. papers34678 2024-06-06T21:05:14.358Z: 1:f72d0350-ccde-593f-b005-4137669c39a8:8:0:0.jpg
- f. papers34678 2024-06-06T21:05:14.358Z: 1:f72d0350-ccde-593f-b005-4137669c39a8:8:1:0.jpg papers34678 2024-06-06T21:05:14.358Z: 1:f72d0350-ccde-593f-b005-4137669c39a8:8:2:0.jpg

- g. papers34678 2024-06-06T21:05:14.358Z: 1:f72d0350-ccde-593f-b005-4137669c39a8:8:3:0~web.mp4
- h. papers34678 2024-06-06T21:05:14.358Z: 1:f72d0350-ccde-593f-b005-4137669c39a8:8:4:0~web.mp4
- i. papers34678 2024-06-06T21:05:14.358Z: 1:f72d0350-ccde-593f-b005-4137669c39a8:8:5:0~web.mp4
- j. papers34678 (Reported) 2024-06-06T21:05:21.642Z: Can I post these & tag you?
- k. papers34678 (Reported) 2024-06-06T21:12:06.144Z: Block me again. I'll post them
- l. liekelewis 2024-06-07T01:17:17.758Z: whered you get those from
- m. liekelewis 2024-06-07T01:19:25.234Z: i wont block you
- n. liekelewis 2024-06-07T01:19:31.369Z: but where did you get those

27. The CyberTip has a total of 6 uploaded files. I reviewed the file associated with CyberTip Report # 196968626. All 6 uploads depicted lascivious behavior but only two are CSAM. Below is the description of the CSAM uploads:

- a. The filename is 1:f72d0350-ccde-593f-b005-4137669c39a8:8:1:0.jpg and the MD5 is 7561968349ddc514df918cdf0ba0e818. The reporting ESP viewed the content and is categorized by ESP as pubescent minor / lascivious exhibition. *The image is of the same pubescent female described above. She is in the bathroom posing in front of the mirror wearing only a black top which she is pulling up exposing both of her breast. She is holding her cell phone in her left hand and is sticking out her tongue. She has little breast development. She is not wearing any underwear or pants but due to the mirror*

appearing wet I am unable to determine if she has any pubic hair. Based on my training and experience, the video as described above depicts CSAM.

- b. The filename is 1:f72d0350-ccde-593f-b005-4137669c39a8:8:0:0.jpg and has an MD5 of f0b9a968841ec1f8fb01dc002a255925. The image is of *the same described pubescent female posing naked in front of her bathroom mirror. She is holding the camera with her left hand and her body is turned sideways exposing her full left breast and part of her right breast.* The reporting ESP viewed the content and is categorized by ESP as pubescent minor / lascivious exhibition. Based on my training and experience, the video as described above depicts CSAM.

Information Obtained Regarding the Subject Premises

28. Checking with the Wisconsin Department of Motor Vehicles, Nolan Pitsch has a valid Wisconsin Driver's License that expires on January 5, 2032, and he resides at 1640 N. Taylor Drive, Sheboygan, Wisconsin. Checking with the Wisconsin Department of Motor Vehicles, Nolan has a black in color 2019 Ford Escape (VIN: 1FMCU9HD9KUA00017) with Wisconsin registration plate 656UGZ that is registered to him. The vehicle is valid and expires November 30, 2024.

29. Research was conducted on Nolan's residence at 1640 N. Taylor Drive (Unit B), City of Sheboygan, Wisconsin. A black 2019 Ford Escape, with Wisconsin registration plates 656UGZ was located on the southwest side of the parking lot that is attached to the apartment building. It should also be noted that a check of the address

on Google Maps, shows a photo from August 2024, displaying the 2019 Ford Escape parked in the lot of 1640 N. Taylor Drive. On September 20, 2024, at approximately 10:15 AM, I observed Nolan Pitsch inside of 1640 N. Taylor Drive (Unit B), in the City of Sheboygan, Wisconsin 53081. See attachment A.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not

actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively,

to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both

show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to

specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of

Internet discussions about the crime; and other records that indicate the nature of the offense.

33. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to

recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography”. For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when

the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

34. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

BIOMETRIC ACCESS TO DEVICES

35. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

36. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

37. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face". During the Trusted Face registration process, the user holds the device in front of his or her face. The

device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

38. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello". During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

39. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

40. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

41. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

42. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of

the aforementioned biometric features, I request authority for law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of any occupants' face of and activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of any occupants' face and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE,
TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH
INTENT TO VIEW CHILD PORNOGRAPHY**

43. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive

materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the

child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.¹

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if NOLAN PITSCHE uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, his vehicle, the SUBJECT PREMISES, or on his person as set forth in Attachment A.

44. Based on the following, I believe that NOLAN PITSCHE, who resides at 1640 N. Taylor Dr, Sheboygan, WI 53081(Unit B), likely displays characteristics common to individuals who distribute, possess or access with intent to view child pornography based on his history of a criminal offense involving minors.

CONCLUSION

45. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

46. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically

evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED:

The entire premises located at 1640 N. Taylor Drive, Unit B, Sheboygan, Wisconsin ("SUBJECT PREMISES"), including any storage or outbuildings and garages, more particularly described as a two-story apartment building, located in the City of Sheboygan, Wisconsin, Sheboygan County, with various shades of brown bricks and white siding, white trim surrounding the exterior windows, white gutters, and dark gray shingles. The front of the apartment faces north east, and the apartment's address "1640" is affixed on four white tiles with units "1640A", "1640B", "1640C", and "1640D" on the east corner of the building and faces to the southeast towards N. Taylor Drive. The front entrance of the SUBJECT PREMISES has a white exterior door with a window. Once inside the front white door, the common area opens up to other units, and immediate to the left is a brown painted door at the bottom of the stairs with brown wood trim, with the letter "B" attached to the upper center of the door. There is an exterior parking lot on the east side of the building. The SUBJECT PREMISES is approximately one tenth of one mile to the north of West Meadows Court and is located on the west side of N. Taylor Drive in the City of Sheboygan.

A black 2019 Ford Escape, with Wisconsin registration plates 656UGZ, which is registered to NOLAN PITTSCH. The Ford Escape has a VIN # of 1FMCU9HD9KUA00017 and has been observed in the parking lot of 1640 N. Taylor Drive, Sheboygan, Wisconsin. Pictures of the residence and vehicle are provided below.







ATTACHMENT B

ITEMS TO BE SEIZED:

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, 18 U.S.C. §§ 2251(a) Sexual Exploitation of a minor/"production" of CSAM and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography):

1. Computers or storage media used to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- A. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- B. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

C. Evidence of the lack of such malicious software;

D. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

E. Evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

F. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

G. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

H. Evidence of the times the COMPUTER was used;

I. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

J. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

K. Records of or information about Internet Protocol addresses used by the COMPUTER;

L. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or

“favorite” web pages, search terms that the user entered in any Internet search engine, and records of user-typed web addresses; and

M. Contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

A. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

B. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

C. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as

microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) and hold up the device(s) to the face of individuals found at the premises to the Touch ID sensor of Android or Apple brand device(s) and the camera of the Apple brand devices, smartphones, or tablets, such as an iPhone or iPad, found at the premises for the purposes of attempting to unlock the device(s) via Touch ID and Face ID in order to search the contents as authorized by this warrant.